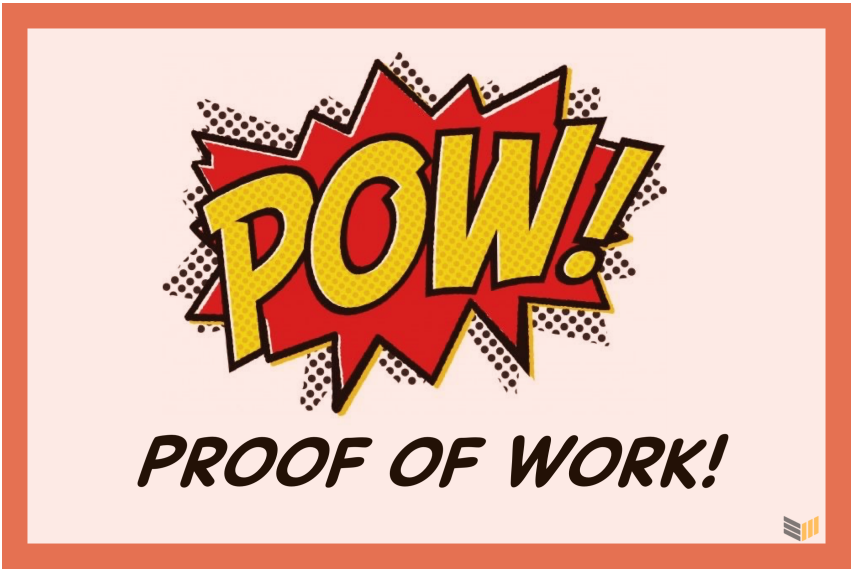
DAY 5: Proof of Work Explained

1 message

Bitcoin Magazine Sun, Aug 21, 2022 at 10:23 PM
<education@bitcoinmagazine.com>
Reply-To: Bitcoin Magazine <education@bitcoinmagazine.com>
To: samglaj3p@gmail.com

You might have heard this term thrown around in the bitcoin space: **PoW.**

PoW reminds me of this old superhero comic:



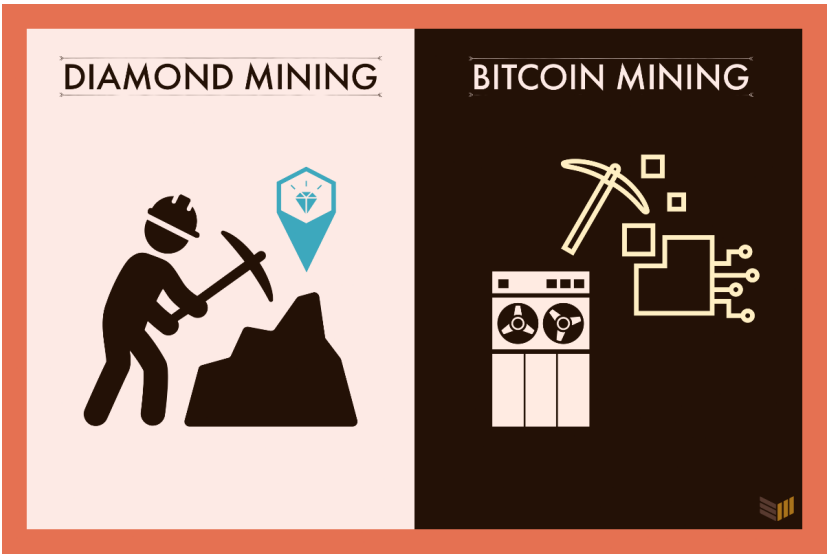
And it's a good symbol, too. Proof of Work really is like a superhero since it allows Bitcoin to work without a centralized controller such as the government. It's the key that unlocks the self-sovereign solution we've been looking for — a computer algorithm that just might fix our financial system.

Here's what it means.

Working Selfishly for the Greater Good

Proof of Work is a consensus algorithm that requires its participants — the Bitcoin miners — to expend energy and computational power in order to lock-in batches of new transactions. In exchange, they are rewarded with bitcoin if they are the first to successfully calculate a difficult 64-character hexadecimal serial number (a hash) that identifies the past transaction history, the new transactions, and their own ID as the winning miner.

In other words, miners want this bitcoin reward for themselves, so they will work tirelessly to try and create a winning solution. The winner then sends their solution and the list of transactions it includes to the blockchain, thus securing those transactions publicly, forever. About every ten minutes, this process repeats itself to help decentralize, secure, and confirm all transactions on the blockchain while rewarding miners for their proof of work.



If very little of that made any sense to you, here's an analogy to help you better understand.

Looking for Diamonds

Diamonds, like bitcoin, are rare. They can't be faked, they're hard to find, and everybody wants one. For the sake of this analogy, we'll just pretend that lab-grown diamonds don't exist.

Imagine that a client wants a diamond of at least a certain size. If you find a diamond that fits the requirement, then you get paid. The bigger the diamonds are, the harder they are to find. Now, because diamonds

are so rare, you need to spend time gathering stones and spend effort breaking into them. It's a luck of the draw — some stones you just throw out, while others can make a diamond ring.

Occasionally, you get lucky and the first ore you break into meets the size requirement. Other times, it takes you much longer to find just a small diamond. But even if you do find several small diamonds, it doesn't matter to the client if none of them are the right size. This is an important point to make for bitcoin mining — that work doesn't *accumulate*. Results are largely based on luck. But, the harder you work, the luckier you may get.

Mining Pools

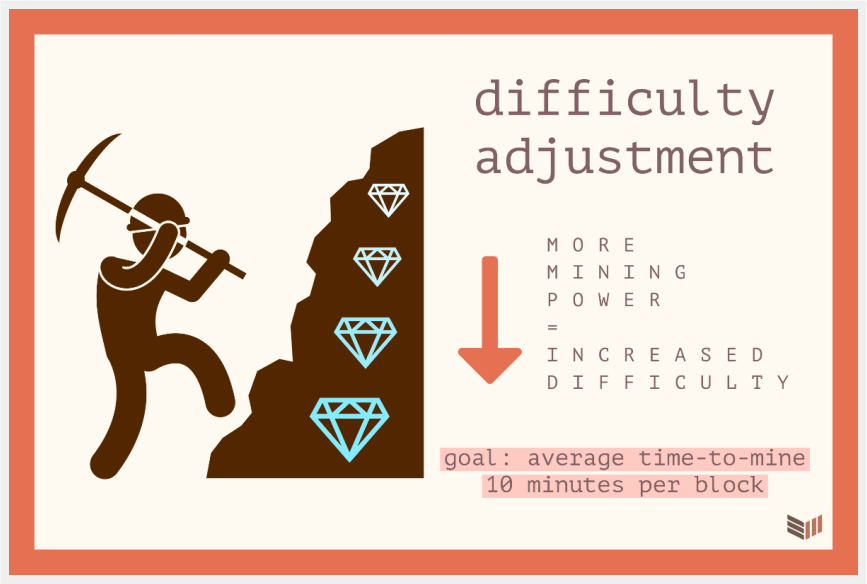
Some miners realize that all this work might be better done as a group effort, so they collaborate and form groups. They decide that if someone in the group finds a diamond big enough for the client, then the entire group gets paid out depending on how much work they've done. They measure the work done by individually weighing the little diamonds that people were able to find against the total.

In Bitcoin, miners come together to form mining pools in a similar way. Bitcoin rewards are distributed within a mining pool depending on how much work the miners have done.

Adjusting for Difficulty

As more people realize that there is money to be made looking for diamonds, the overall number of participants increases, which thereby increases the likelihood of someone finding a diamond of the right size quickly.

Well, let's say that every two weeks, the client takes note of how long it took to find a diamond of a certain size. If there are more people working and it takes less time on average to find the diamonds, then the size requirements for the diamonds get bigger for the next two weeks. Because larger diamonds are rarer, it becomes much harder for someone to find a diamond if the size requirements get bigger, and vice versa.



The Bitcoin protocol has a built-in difficulty adjustment. Every 2016 blocks (about two weeks), the difficulty to mine bitcoin adjusts as more miners either come online or go offline. If there is more computational power working to solve the hash, then it becomes more difficult to find a winning solution. If miners come offline for some reason (like after China banned miners), then it becomes easier for miners who are still online to mine bitcoin.

The goal is to ultimately find equilibrium and issue new bitcoin at a steady rate — an average of ten minutes per new block. You can track how difficulty adjusts here: https://btc.com/stats/diff

Tomorrow, we'll go over more of what bitcoin mining looks like and how the network distributes new bitcoin over time.

Do you have any questions so far? Tweet them using the hashtag **#21DaysofBitcoin** to get some answers from a community of expert bitcoiners!

Bitcoin 2023 Conference

Take 10% off your Bitcoin 2023 conference tickets. Join us for the world's largest bitcoin conference.
Promo code **"21DAYS"**

Bitcoin Magazine Store

Take 21% off our collection of bitcoin shirts, hats, or mugs from the official Bitcoin Magazine store.
Promo code: **"STORE21D"**

Bitcoin Magazine Print

Take $12 off your annual print subscription. Get 4 issues/year to your mailbox, starting with The Censorship Resistant Issue.
Promo code: **"21DAYS"**